

1 What is claimed is:

2

3 1. A cryptographic communication method wherein
4 when different encryption algorithms are operated at a
5 transmission side and a reception side, the transmission
6 side encrypts an encryption algorithm operated at the
7 transmission side with an encryption algorithm operated
8 at the reception side and transmits the encrypted
9 algorithm to the reception side.

10

11 2. A cryptographic communication method wherein
12 information on an encryption algorithm operated at a
13 transmission side and information on an encryption
14 algorithm operated at a reception side are obtained from
15 the transmission side and when different encryption
16 algorithms are operated at the transmission side and the
17 reception side, an encryption algorithm operated at the
18 transmission side is encrypted with an encryption
19 algorithm operated at the reception side and transmitted
20 to the reception side.

21

22 3. A cryptographic communication method as
23 claimed in claim 2 wherein signature data produced based

1 on a public key preliminarily allocated to the
2 transmission side is supplied to the reception side with
3 said encryption algorithm operated at the transmission
4 side with the encryption algorithm operated at the
5 reception side.

6

7 4. A cryptographic communication method as
8 claimed in claim 2 wherein signature data produced based
9 on a public key preliminarily allocated to the
10 transmission side is supplied to the transmission side
11 together with said encryption algorithm operated at the
12 transmission side encrypted with the encryption
13 algorithm operated at the reception side and transmitted
14 to the reception side.

15

16 5. An encryption algorithm sharing management
17 method for sharing an encryption algorithm for
18 cryptographic communication, comprising the steps of:
19 from a user of a transmission side, obtaining a
20 user identifier indicating the user of the transmission
21 side and a user identifier indicating a user of a
22 reception side; and
23 querying a data base in which user identifiers

1 indicating users and their corresponding encryption
2 algorithms are preliminarily described, so as to obtain
3 an encryption algorithm operated by the user of the
4 transmission side and an encryption algorithm operated
5 by the user of the reception side,
6 wherein if said encryption algorithm operated by
7 the user of the transmission side is different from said
8 encryption algorithm operated by the user of the
9 reception side, data indicating said encryption
10 algorithm operated by the user of the transmission side
11 is encrypted with said encryption algorithm operated by
12 the user of the reception side and transmitted to the
13 user of the reception side.

14

15 6. An encryption algorithm sharing management
16 method for sharing an encryption algorithm for
17 cryptographic communication, comprising the steps of:

18 from a user of a transmission side, obtaining a
19 user identifier indicating the user of the transmission
20 side and a user identifier indicating a user of a
21 reception side;

22 querying a data base in which user identifiers
23 indicating users, corresponding encryption algorithms

1 and encryption keys thereof, are preliminarily described
2 so as to obtain an encryption algorithm operated by the
3 user of the transmission side and an encryption key
4 thereof and an encryption algorithm operated by the user
5 of the reception side and an encryption key thereof,
6 wherein if said encryption algorithm operated by
7 the user of the transmission side is different from said
8 encryption algorithm operated by the user of the
9 reception side, data indicating said encryption
10 algorithm operated by the user of the transmission side
11 and an encryption key produced based on the encryption
12 key operated by the user of the reception side
13 corresponding to a key length of said encryption
14 algorithm operated by the user of the transmission side
15 is encrypted with said encryption algorithm operated by
16 the user of the reception side and transmitted to the
17 user of the reception side.

18

19 9. A network communication system composed by
20 connecting a plurality of users, comprising at least one
21 encryption key management station to be connected from a
22 user of a transmission side,

23 said encryption key management station obtaining,

1 from the user of the transmission side, information
2 indicating an encryption algorithm operated by the user
3 of the transmission side and information indicating an
4 encryption algorithm operated by a user of a reception
5 side and if different encryption algorithms are operated
6 by the user of the transmission side and the user of the
7 reception side, encrypting the encryption algorithm
8 operated by the user of the transmission side with the
9 encryption algorithm operated by the user of the
10 reception side and transmitting it to the user of the
11 reception side.

12

13 10. A network communication system composed by
14 connecting a plurality of users, comprising at least one
15 encryption key management station to be connected from a
16 user of a transmission side,

17 said encryption key management station comprising a
18 data base in which a correspondence between a user
19 identifier indicating a user and an encryption algorithm
20 operated by said user is preliminarily described about
21 each user;

22 wherein when a communication is carried out from
23 the user of the transmission side to a user of a

1 reception side, a user identifier indicating the user of
2 the transmission side and a user identifier indicating a
3 user of a reception side are obtained from the user of
4 the transmission side and said data base is queried with
5 the obtained identifiers as a key so as to obtain an
6 encryption algorithm operated by the user of the
7 transmission side and an encryption algorithm operated
8 by the user of the reception side, and
9 if the encryption algorithm operated by the user of
10 the transmission side is different from the encryption
11 algorithm operated by the user of the reception side,
12 the encryption algorithm operated by the user of the
13 transmission side is encrypted with the encryption
14 algorithm operated by the user of the reception side and
15 transmitted to the user of the reception side.

16

17 11. An encryption algorithm sharing management
18 method for sharing an encryption algorithm for
19 cryptographic communication, comprising the steps of:

20 from a user of a transmission side, obtaining a
21 user identifier indicating the user of the transmission
22 side and a user identifier indicating a user of a
23 reception side; and

1 querying a data base in which user identifiers
2 indicating users and their corresponding encryption
3 algorithms, are preliminarily described so as to obtain
4 an encryption algorithm operated by the user of the
5 transmission side and an encryption algorithm operated
6 by the user of the reception side;
7 wherein if said encryption algorithm operated by
8 the user of the transmission side is different from said
9 encryption algorithm operated by the user of the
10 reception side, data indicating said encryption
11 algorithm operated by the user of the reception side is
12 encrypted with said encryption algorithm operated by the
13 user of the transmission side and transmitted to the
14 user of the transmission side.
15
16 12. An encryption algorithm sharing management
17 method for sharing an encryption algorithm for
18 cryptographic communication, comprising the steps of:
19 from a user of a transmission side, obtaining a
20 user identifier indicating the user of the transmission
21 side and a user identifier indicating a user of a
22 reception side;
23 querying a data base in which user identifiers

1 indicating users, corresponding encryption algorithms
2 and encryption keys thereof, are preliminarily described
3 so as to obtain an encryption algorithm operated by the
4 user of the transmission side and an encryption key
5 thereof and an encryption algorithm operated by the user
6 of the reception side and an encryption key thereof,
7 wherein if said encryption algorithm operated by
8 the user of the transmission side is different from said
9 encryption algorithm operated by the user of the
10 reception side, data indicating said encryption
11 algorithm operated by the user of the reception side and
12 an encryption key produced based on the encryption key
13 operated by the user of the transmission side
14 corresponding to a key length of said encryption
15 algorithm operated by the user of the reception side is
16 encrypted with said encryption algorithm operated by the
17 user of the transmission side and transmitted to the
18 user of the transmission side.

19

20 15. A network communication system composed by
21 connecting a plurality of users, comprising at least one
22 encryption key management station to be connected from a
23 user of a transmission side,

1 said encryption key management station obtaining,
2 from the user of the transmission side, information
3 indicating an encryption algorithm operated by the user
4 of the transmission side and information indicating an
5 encryption algorithm operated by a user of a reception
6 side, and if different encryption algorithms are
7 operated by the user of the transmission side and the
8 user of the reception side, encrypting the encryption
9 algorithm operated by the user of the reception side
10 with the encryption algorithm operated by the user of
11 the transmission side and transmitting it to the user of
12 the transmission side.

13

14 16. A network communication system composed by
15 connecting a plurality of users, comprising at least one
16 encryption key management station to be connected from a
17 user of a transmission side,

18 said encryption key management station comprising a
19 data base in which a correspondence between a user
20 identifier indicating a user and an encryption algorithm
21 operated by said user is preliminarily described about
22 each user;

23 wherein when a communication is carried out from

1 the user of the transmission side to a user of a
2 reception side, a user identifier indicating the user of
3 the transmission side and a user identifier indicating a
4 user of a reception side are obtained from the user of
5 the transmission side, and said data base is queried
6 with the obtained identifiers as a key so as to obtain
7 an encryption algorithm operated by the user of the
8 transmission side and an encryption algorithm operated
9 by the user of the reception side, and
10 if the encryption algorithm operated by the user of
11 the transmission side is different from the encryption
12 algorithm operated by the user of the reception side,
13 the encryption algorithm operated by user of the
14 reception side is encrypted with the encryption
15 algorithm operated by the user of the transmission side
16 and transmitted to the user of the transmission side.
17
18 17. A cryptographic communication method wherein
19 if different encryption algorithms are operated by a
20 transmission side and a reception side, an encryption
21 algorithm operated by the reception side is encrypted
22 with an encryption algorithm operated by the
23 transmission side and transmitted to the transmission

1 side.

2

3 18. A cryptographic communication method wherein
4 information indicating an encryption algorithm operated
5 by a transmission side and information indicating an
6 encryption algorithm operated by a reception side are
7 obtained from the transmission side and when different
8 encryption algorithms are operated by the transmission
9 side and the reception side, the encryption algorithm
10 operated by the reception side is encrypted with the
11 encryption algorithm operated by the transmission side
12 and transmitted to the transmission side.

13

14 19. A cryptographic communication method as
15 claimed in claim 18 wherein signature data produced
16 based on a public key preliminarily allocated to the
17 reception side is supplied to the transmission side with
18 the encryption algorithm operated by the reception side
19 encrypted with the encryption algorithm operated by the
20 transmission side.

21

22 20. An encryption algorithm sharing management
23 method for sharing an encryption algorithm for

1 cryptographic communication, comprising the steps of:
2 from a user of a transmission side, obtaining a
3 user identifier indicating the user of the transmission
4 side and a user identifier indicating a user of a
5 reception side;
6 querying a data base in which user identifiers
7 indicating users and corresponding encryption algorithms
8 are preliminarily described so as to obtain an
9 encryption algorithm operable by the user of the
10 transmission side and an encryption algorithm operable
11 by the user of the reception side;
12 determining whether or not there is an encryption
13 algorithm operable by the user of the transmission side
14 and the user of the reception side commonly; and
15 if the commonly operable encryption algorithm
16 exists, the user of the transmission side is notified
17 that cryptographic communication at the user of the
18 transmission side and the user of the reception side is
19 enabled.
20
21 21. An encryption algorithm sharing management
22 method as claimed in claim 20 wherein:
23 if the commonly operable encryption algorithm

1 exists, information indicating the commonly operable
2 encryption algorithm is transmitted to the user of the
3 transmission side and
4 if the commonly operable encryption algorithm does
5 not exists, the user of the reception side is notified
6 that cryptographic communication at the user of the
7 transmission side and the user of the reception side is
8 disabled.

9

10 22. An encryption algorithm conversion method for
11 converting a first encryption algorithm to a second
12 encryption algorithm comprising:

13 querying a data base in which user identifiers
14 indicating users, corresponding encryption algorithms
15 and encryption keys thereof, are preliminarily described
16 for a user, whose encryption algorithm is to be
17 converted as a key, so as to obtain a first encryption
18 algorithm operated by the user whose encryption
19 algorithm is to be converted and a first encryption key
20 thereof; and

21 with a first management secret key preliminarily
22 allocated for management and applied to the first
23 encryption algorithm, supplying first and second

1 signature data for the first encryption key and a second
2 encryption key, public key data obtained by encrypting a
3 second public key corresponding to a second management
4 secret key applied to a second encryption algorithm
5 preliminarily allocated for management with the first
6 encryption algorithm, the second encryption algorithm
7 encrypted with the first encryption algorithm and
8 signature data produced based on the second management
9 secret key to the user whose encryption algorithm is to
10 be converted.

11

12 23. A cryptographic communication method wherein
13 information concerning a first encryption algorithm is
14 encrypted with a second encryption algorithm, and
15 encrypted information including said information
16 concerning said first encryption algorithm is
17 transmitted from a first side to a second side, or from
18 said second side to said first side.

19

20 24. A terminal device for transmitting or
21 receiving information, where said terminal device
22 encrypts information concerning a first encryption
23 algorithm with a second encryption algorithm, and

- 1 transmits or receives encrypted information including
- 2 said information concerning said first encryption
- 3 algorithm.